REMARKS

Claims 1 and 22-28 are pending, and claims 2-21 have been canceled.

A. **Claims 1-21 were rejected under 35 U.S.C. §103(a) as being anticipated by Holloway et al. (US 5,805,801) in view of Sofer et al. (US 5,489,896).** The applicant respectfully traverses this rejection for the following reason(s).

It is not clear why the Examiner is again rejecting claims 2-21, which were previously canceled. We do not understand why the Examiner has again applied a rejection of "anticipation" under §103(a). These errors were noted in our reponse filed on 13 September 2006.

We will again assume the rejection is for claims 1 and 22-28, since claims 2-21 have been canceled, and the Examiner meant "obvious" instead of "anticipated".

Holloway's invention relates to systems and methods for detecting and preventing intrusion into a campus local area network by an unauthorized user. A managed hub discovers each interconnect device in the network that supports the security feature and maintains an interconnect device list of such devices, which may include token ring switches, Ethernet switches, bridges and routers. The managed hub determines the interconnect devices in the campus network that are capable of supporting a local area network (LAN) security feature. The managed hub then uses the responses to build and maintain a table of interconnect devices in the network that support the security feature. Here, during a discovery phase, the managed hub periodically sends a discovery

frame to a LAN security feature group address. The managed hub detects an intrusion by an unauthorized address on one of its ports by comparing the MAC addresses on each port against a list of authorized MAC addresses, disables the port and notifies the other interconnect devices in the network of the intrusion by transmitting a security breach detected frame to the LAN security feature group address. The interconnect devices set a filter on their respective ports against the intruding unauthorized address.

Sofer's invention relates to a security unit for a network having a data bus to which a plurality of stations (interconnect devices) can be connected wherein the security unit monitors traffic on the data bus and only enables authorized data to flow along the data bus. The data bus and the security unit are part of a hub. The traffic includes a multiplicity of data packets each having source and destination addresses and the security unit includes a plurality of correlators for determining that the source and destination addresses indicate an authorized communication. Additionally, each station is connected to the data bus via a port having a port address and one of the correlators correlates the source address with an authorized port address.

Note that Sofer's port address is not the same nor equivalent to a destination address, as Sofer clearly differentiates the two addresses. A destination address is the final destination for the message, where the port address is for a particular port connected to the final destination.

Sofer differs from Holloway in that Sofer teaches the destination station address be in a list of authorized destination station addresses for the source station address, because Sofer is concerned with permitting two stations being authorized to communicate with each other. Holloway is only concerned with intrusion by an unauthorized source station outside the network breaking into the

network via one of the ports. There is no concern with whether a source station is authorized to connect to a destination station.

If one of ordinary skill in the art were motivated to modify the security of a network utilizing Holloway's system in the manner taught by Sofer, then the skilled artisan would modify the system as taught by Sofer.

Sherer's invention relates to a method and apparatus for providing secure network communications on a per-packet level in a network system. According to Sherer, adaptor cards or drivers for installation in a network include a simple data pattern enforcer (DPE) operating at the lowest layer at which packets are recognized. The DPE may be comprised of hardware or software elements and have associated with it a mechanism for applying a rule or a set of rules to packets either transmitted or received at the lowest layer at which the packets exist. These mechanisms may include a set of one or more pattern-matching masks and a count indication into the packet as to where pattern-matching will begin.

Up to three values are used by the data pattern enforcer (DPE): a Count, a Value Bit Vector (VBV), and a Don't Care Bit Vector (DCBV). The count is a value indicating a position in a network data packet. For example, the count may represent a number of bytes into a network packet. The VBV is a bit string that is compared to the bits in the packet at the position indicated by the count. The DCBV, if present, is a mask indicating whether or not certain bit locations within the VBV are values that are not used by the matching. If a DCBV is used, for every bit in the VBV there is a Don't Care Bit (DCB) indicating whether that bit is used or ignored in the compare.

For example, if VBV=01101110, DCBV=10000001 and Count=4 , then when a packet is

received off the network, the byte indicated by the count is examined. The data pattern enforcer (DPE) expects the data to be of the format x110111x, where x indicates don't-care bit positions (either 0 or 1) and the other values match what is in a VBV register. The examined byte may be a byte in a packet header, either part (source or destination) of a MAC address, the IPX address, or the IP address. However, Sherer's invention allows verification to happen at any place in the packet as determined by the count value.

The present invention has an advantage over the applied art, because of its use of access vectors. An access vector has been defined by the specification to consist of a bit vector. The bit value "0" means restriction to access and "1" means allowance for access. For example, if a server node S1 has an access vector 00010000 and a client node C1 has access vector 10000001, then client node (source station) C1 cannot access server node (destination station) S1, but another client node C2 having access vector 00010001 can access server node S1.

For further understanding, access vector 00010000 of a server node S1 means that S1's HostID is 3, and its access vector is 0x80>>3. If C1 is going to be an access client node, the access vector of C1 should be (0x80>>3). If the access vector of C1 is 10010001, then this access vector 10010001 means C1 can access server nodes that have HostID 0, 3 or 7. Thus a client node having an access vector xxx1xxxx (x can be a 0 or 1) can access a server node having a HostID of 3, and a client node having an access vector xxx0xxxx (x can be a 0 or 1) is restricted from accessing a server node having a HostID of 3.

Accordingly, it is possible to use the same (e.g., 8-bit) access vectors for more than one (32-

bit) source address and (32-bit) destination address, thereby saving memory space for storing the correlating 8-bit access vectors instead of correlating each 32-bit source address and destination address.

Claim 1

Claim 1 is directed to a MAC (media access control) address-based communication restricting method using **access vectors stored in address tables**, wherein the access vectors indicate whether two nodes, corresponding to a MAC source address and a MAC destination address, may access each other, the method calls for, in part:

detecting, in the address table, access vectors corresponding to the MAC destination and source addresses.

The combination of applied art fails to teach the foregoing feature.

Contrary to the Examiner's remarks, neither Holloway nor Sofer teach *access vectors*, much less *access vectors stored in address tables*. The Examiner is respectfully requested to identify where the phrase "access vectors" is found in both Holloway and Sofer.

Note that the phrase "access vectors" are defined by the specification, and it is an error for the Examiner to give them a different definition. During examination, the claims must be interpreted as broadly **as their terms <u>reasonably</u> allow**. This means that the words of the claim must be given their plain meaning **<u>unless applicant has provided a clear definition in the specification</u>**. See MPEP §2111.01; and *Toro Co. v. White Consol. Indus., Inc.*, 199 F.3d 1295, 1299, 53 USPQ2d 1065, 1067 (Fed. Cir. 1999)("[W]ords in patent claims are given their ordinary meaning in the usage

of the field of the invention, unless the text of the patent makes clear that a word was used with a special meaning.").

Although Sherer does teach a Value Bit Vector (VBV), this VBV is not an access vector stored in an address table, but instead is an 8-bit value stored in a register. See Fig. 6, registers 95 and 95a of rule sets 98 and 98a, respectively.

Accordingly, Sherer does not teach *access vectors stored in address tables*.

Therefore, the rejection of claim 1 is deemed to be in error and should be withdrawn.

The VBV in Sherer is simply an 8-bit value that should appear somewhere (corresponding to a stored count value stored in a count register 93 or 93a of rule sets 98 and 98a, respectively) in a received data packet. According to the count value, a byte of received data corresponding to the location identified by the count value is compared with the VBV to determine if the received packet should be discarded or received.

Claim 1 requires that a MAC destination address and a MAC source address included in the received packet data be read, and that the access vectors corresponding to the MAC destination and source addresses the address table be detected. Upon detection of **both** the access vector corresponding to the MAC destination address and the access vector corresponding to the MAC source address. Then the access vector corresponding to the MAC destination address is compared to the access vector corresponding to the MAC source address. The two nodes (preamble),

corresponding to the MAC source address and the MAC destination address are denied access to each other if the access vectors of the MAC destination and source addresses are not matched.

Sherer does not teach comparing two VBV's to each other.

Sherer does not teach comparing an access vector corresponding to a received MAC destination address to an access vector corresponding to a received MAC source address, i.e., *reading a MAC destination address and a MAC source address included in the received packet data;* and *detecting, in the address table, access vectors corresponding to the MAC destination and source addresses.*

Sherer does not teach *denying* [two nodes] *access* [to each other] *if the access vectors of the MAC destination and source addresses are not matched.* See preamble and last feature of claim 1.

Instead Sherer teaches accepting or rejecting a received data packet.

Therefore, the rejection of claim 1 is deemed to be in error and should be withdrawn.

Further, the Applicant has asserted that the use of access vectors instead of MAC destination and source addresses for comparison is advantageous over the art. The Examiner has not addressed the asserted advantage. See MPEP §707.07(f).

Claims 22-28 are deemed to be non-obvious and patentable over the art of record for the same reasons as claim 1.

The Examiner is respectfully requested to reconsider the application, withdraw the objections and/or rejections and pass the application to issue in view of the above amendments and/or remarks.

Should a Petition for extension of time be required with the filing of this Amendment, the Commissioner is kindly requested to treat this paragraph as such a request and is authorized to charge Deposit Account No. 02-4943 of Applicant's undersigned attorney in the amount of the incurred fee if, **and only if**, a petition for extension of time be required **and** a check of the requisite amount is not enclosed.

Respectfully submitted,

Robert E. Bushnell
Attorney for Applicant
Reg. No.: 27,774

1522 K Street, N.W.
Washington, D.C. 20005
(202) 408-9040

Folio: P56339
Date: 2/28/07
I.D.: REB/MDP